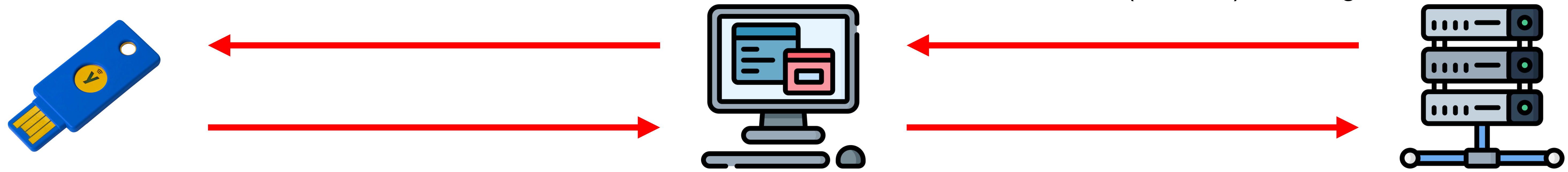

2. RP ID, credential ID, clientDataHash

1. credential ID, (random) challenge

authenticator

4. authenticatorData, **signature**

client/platform

5. **signature**, clientDataJSON,
authneticatorData,

relying party

RP ID: example.com

🔑 public key

3. lookup credential (and its **private key** 🗝) by RP ID and credential ID

4. signature = **sign(** hash(authenticatorData || clientDataHash) , 🗝 **private key** **)**

6. clientDataHash = compute from clientDataJSON

6. expectedHash = hash(authenticatorData || clientDataHash)

7. result = **verify(** expectedHash, 🔑 public key signature **)**